العنوان:	الجرائم المعلوماتية والدليل الجنائي مسميات وخصائص وإبعاد اجتماعية وأمنية وصحية
المصدر:	المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية
المؤلف الرئيسي:	اليوسف، عبدالله بن محمد
محكمة:	نعم
التاريخ الميلادي:	2015
مكان انعقاد المؤتمر:	المملكة العربية السعودية. الرياض
رقم المؤتمر:	1
الهيئة المسؤولة:	جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات
الشهر:	نوفمبر
الصفحات:	95 - 113
رقم MD:	690611
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	HumanIndex
مواضيع:	الجرائم المعلوماتية
رابط:	http://search.mandumah.com/Record/690611

الجرائم المعلوماتية والدليل الجنائي
مسميات وخصائص وأبعاد اجتماعية وأمنية وصحية

عميد م عبد الله بن محمد اليوسف

خبير أدلة جنائية ومدير معهد علوم الأدلة الجنائية سابقاً

الأمن العام – وزارة الداخلية

الرياض، المملكة العربية السعودية

الملخص-نلاحظ أنه هناك توجه عام لتعاملات الإليكترونية لكلا القطاعين الخاص والعام ويهمنا هنا على مستوى الجهات الحكومية والورقة العلمية هنا تم استعراضها وفق ثلاثة محاور.

المحور الأول: مفهوم الجرائم المتصلة بالحاسب، جرائم السرقة المتعلقة بالحاسب، من يرتكب جرائم الحاسب، خصائص الجرائم المتصلة بالحاسب، أمن العمليات، التعامل مع جرائم الحاسب، تعريف نظام التعاملات الإلكترونية السعودي، مكافحة جرائم تقنية المعلومات في المملكة، أهداف نظام مكافحة جرائم تقنية المعلومات في المملكة، ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية، المؤتمر السعودي للصحة الإلكترونية، سياسة حجب المواقع – وحدة الخدمات الإليكترونية – مدينة الملك عبد العزيز للعلوم والتقنية، الرقابة الذاتية / تقويم للسلوك.

أما المحور الثاني: مواقع التواصل الاجتماعية بين الإيجابيات والسلبيات من منظور وأبعاد اجتماعية ونفسية، مسميات وأنواع وخصائصها، من منظور وأبعاد شرعية /كشفت وسائل التواصل الاجتماعي ما في المجتمعات من خلل في التدين، وضعف في التربية، وانحطاط في الأخلاق، وسائل التواصل الاجتماعي ابتلاء من الله تعالى لعبادة، من منظور صحي، والإدمان وأمراض نفسية عصرية، قلق وعدم استقرار، حيرة، عصبية وغيرها. ومن منظور وأبعاد أمنية، القرصنة، الإرهاب المعلوماتي مجالات نشاط الإرهاب المعلوماتي، جرائم الإرهاب المعلوماتي، صناعة ونشر الفيروسات، تعطيل وشلل أجهزة الحاسوب. الدخول الغير مصرح، انتحال الشخصية، المضايقة والملاحقة – التغرير والاستدراج، التشهير وتشويه السمعة، صناعة ونشر الإباحية – النصب والاحتيال. الطرق لحماية الشباب من وسائل التغرير التي تستهدفهم وتستهدف استقطابهم. تحصين الشباب، تكوين جمعيات مجتمع مدني تطوعية، انخفاض تقدير الذات، حرية التعبير.

أما المحور الثالث : علم الأدلة الرقمية، التحديات علم الأدلة الرقمية، أولاً – التحديات العامة، ثانياً – التحديات التقنية، ثالثاً – تحديات الموارد البشرية، رابعاً – التحديات العامة / علم التحقيق في الأدلة الرقمية، أهمية علم التحقيق في الأدلة الرقمية، خصائص التحقيق في الأدلة الرقمية تعريف علم التحقيق في الأدلة الرقمية: مسرح الجريمة في الجريمة الإلكترونية، أنواع الأدلة الرقمية وأشكاله خصائص الأدلة الرقمية، مميزات الأدلة الرقمية ، نطاق العمل بالدليل الرقمي خبراء الأدلة الرقمية، ومتطلبات خبراء الأدلة الرقمية، الهواتف النقالة، أماكن العثور على الأدلة الإلكترونية / الأدلة الرقمية في الهواتف النقالة / – تخزين البيانات في (3) مواقع / شريحة الاتصال –كرت الذاكرة – خواص أجهزة الهواتف النقالة مركز الإنتربول لمكافحة الجريمة الرقمية، الاستفادة من الأدلة الجنائية الرقمية.

1- مدخل

نلاحظ أنه هناك توجه عام لتعاملات الإليكترونية لكلا القطاعين ويهمنا هنا على مستوى الجهات الحكومية وفق الأوامر السامية التالية : وجه تعميم رئيس مجلس الوزراء رقم (7/ ب/ 26345) وتاريخ 19/ 12/ 1422 هـ، الجهات الحكومية ببناء قواعد معلومات لإعمالها للاستفادة منها في تسهيل التعاملات مع الأجهزة الحكومية الأخرى وفي إعداد التقارير السنوية عن أعمال الجهة.

كما جاء في الفقرة "خامساً" من تعميم رئيس مجلس الوزراء المشار إليه أعلاه، نصها: "خامساً: على الجهات الحكومية بناء قواعد معلومات تعتمد عليها في أعمالها، وتسهل التعامل مع الأجهزة الحكومية الأخرى، ويستفاد منها في إعداد التقارير السنوية.

– ويوضح هذا التعميم دعم وتوجيه القيادة للجهات الحكومية لإدارة أعمالها إلكترونياً.

وهو ما يؤكد التوجه نحو تطبيق مفهوم التعاملات الإلكترونية الحكومية من خلال تبني الجهات الحكومية الأنظمة المعلوماتية وبناء قواعد البيانات التي تساعد في تطوير أساليب إدارة المرافق الحكومية، ورفع مستوى الدقة والإنتاجية في هذا المجال والتعامل مع الأجهزة الحكومية الأخرى إلكترونياً مما يسهل تكامل البيانات بين الأجهزة الحكومية وبالتالي :– إتاحة إمكانية تبادل البيانات وتوفير الإحصائيات والمعلومات الدقيقة على مستوى الجهات الحكومية وإعداد التقارير السنوية عن أعمال الجهات الحكومية إلكترونياً، وكما جاء في (قرار مجلس الوزراء رقم (235) وتاريخ 20/ 8/ 1425 هـ) التحول من الوسائل التقليدية إلى الإلكترونية.

كما وجه مجلس الوزراء (بالقرار رقم 8189 / م ب وتاريخ 19/ 6/ 1426 هـ) الجهات الحكومية بتشكيل لجان داخلية للتعاملات الإلكترونية الخاصة – بها، كما أقر مجلس الوزراء الموقر في جلسته يوم الإثنين 7 ربيع الأول 1428 هـ برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز – حفظة الله – نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، الخطة الوطنية للاتصالات وتقنية المعلومات :-

وتم الانتهاء من إعداد مشروع الخطة الوطنية للاتصالات وتقنية المعلومات وهي في طور الإقرار حالياً، حيث اشتملت على منظور بعيد المدى لتقنية المعلومات في المملكة للعشرين سنة القادمة، متكوناً :

من رؤية مستقبلية، وسبعة أهداف عامة، وعدد من سياسات التنفيذ بالإضافة إلى الخطة إلى الخطة الخماسية الأولى لتقنية المعلومات، شاملة أهدافاً محددة مشتقة من المنظور بعيد المدى، ومن سياسات تنفيذ، ومقترحات لعدد من المشاريع والتنظيمات والإجراءات الخماسية الأولى لتقنية المعلومات، شاملة أهدافاً محددة مشتقة من المنظور بعيد المدى، ومن سياسات تنفيذ، ومقترحات لعدد من المشاريع والتنظيمات والإجراءات. فالجريمة المعلوماتية قوامها أحد السببين التاليين :- أن تكون المعلوماتية، وسيلة للغش والتحايل والاعتداء.

* أن تكون المعلوماتية نفسها محلاً للاعتداء.

توصيف الجريمة :

اشتقت كلمة الجريمة في اللغة من الجرم وهو التعدي أو الذنب، وجمع الكلمة إجرام وجروم وهو الجريمة. وقد جرم يجرم واجترم وأجرم فهو مجرم وجريم [1] والجريمة الإلكترونية هي " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها" [2]. وتتمثل الجريمة الإلكترونية في كل فعل أو سلوك سيء غير مشروع مرتبط بأجهزة الحاسب الآلي مما قد يسبب خسارة للمجني عليه وإمكانية حصول مرتكب هذه الجريمة على أية ربح أو مكسب. وغالباً ما تهدف هذه الجرائم الإلكترونية إلى الحصول على معلومات سرية أو تغيير وتزوير بعض المعلومات أو حتى إفساد الأجهزة الإلكترونية وتعطيلها.

2- المحور الأول

مفهوم الجرائم المتصلة بالحاسب [3]

لقد أصبحت تكنولوجيا المعلومات تشكل جزءاً أساسياً من الحياة اليومية. وأصبحت الحاسبات أداه منتشرة لا يمكن الاستغناء عنها (indispensable) في المجتمعات الصناعية، كما أن تأثيرها على محتوى، وشكل، ووقت، ومجال النشاطات اليومية.

جرائم السرقة المتعلقة بالحاسب

تعد نمطاً حديثاً من أنماط الجريمة لم تعرفها إلا المجتمعات المعاصرة. فقد أدى الاستخدام الواسع لأجهزة الحاسب في المعاملات الحكومية المدنية العسكرية والمعاملات التجارية إلى دفع بعض الأشخاص إلى الاستفادة غير القانونية على هذا المنتج.

ويمكن تعريف الجريمة المتصلة بالحاسب بأنها : ((أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أو موضوع للجريمة ويمكن تقسيم جرائم الحاسب إلى نوعين :

1- الحاسب كأداة في الجريمة.

2- الحاسب كهدف للجريمة.

1) الحاسب كأداة في الجريمة

من الأمثلة على استخدام الحاسب كأداة للجريمة سرقة الخدمات وبذلك أن يقوم مجرم الحاسب بالاستخدام غير القانوني للحاسب أو استخدام الحاسب قانونياً ولكن لأغراض غير مسموح بها بما في ذلك الدخول غير القانوني على نظام الحاسبات الخاصة، (سرقة المعلومات).

العمليات المالية غير القانونية :

أ- كالدخول على حسابات العملاء وتحويلها إلى حساب شخصي أو سرقتها.

ب- بالإضافة إلى سرقة الممتلكات عن طريق الحاسب.

ت- أو نقل ملكيتها عن طريق الحاسب بطريقة غير شرعية.

([1]) ابن منظور، لسان العرب.

([2]) محمد محمود مندورة، جرائم الحاسب الآلية. الرياض: مكتب الآفاق المتحدة، 1410 هـ.

([3]) الظواهر الإجرامية المستحدثة وسبل مواجهتها مقتطفات من البحث الثالث: جرائم الحاسب والإنترنت د. ذياب موسى البداينة – باختصار وتصرف.

2) أما الحاسب كهدف للجريمة

أما الفئة الثانية فتشمل سرقة مكونات الحاسب الفيزيقية أو البرمجيات أو إعادة تصنيعها وبيعها عادة بأسعار رخيصة.

ومن أمثلة جرائم الحاسب ما يلي :

أ/ القيام بفتح حساب في البنك من قبل موظف البنك وتحويل مبلغ معين (زهيد) من حسابات المودعين حيث لا يهتم المودع لهذا المبلغ نظراً لقلته.

ب/ استخدام كلمة السر للمسؤولين من الجامعات أو كبرى الشركات والدخول على نظام الحاسب وتغيير الدرجات للطلبة.

من يرتكب جرائم الحاسب / تصنيف مرتكبي جرائم الحاسب إلى ثلاث فئات :

القراصنة (crackers)

والقراصنة جماعة فريدة، وتاريخياً فقد كان الحافز بوصفهم متحدين وهم يعملون في جماعات أو بشكل فردي، ولكن غالبيتهم يعملون بشكل فردي.

مجرمو الحاسب – (computer criminals)

ويمكن أن تعد الفئات في المجموعات الثلاث سابقة الذكر ((فئات مجرمين)).

أ/ التجسس (Espionage)

تقدم الحاسبات في عالم اليوم العديد من المهام الحساسة والمتعلقة بكافة الأنشطة الاقتصادية والعسكرية والوطنية ... إلخ، وتنقل مثل هذه المعلومات لدول أخرى أو بالتعاون معها.

ب/ الاحتيال وسوء الاستخدام (Fraud & Aduse).

يعد سوء الاستخدام والاحتيال في الحاسب من الجرائم المتزايدة، فقد انتقلت غالبية جماعات الجريمة المنظمة والمحلية والدولية إلى جرائم الحاسب كمصدر للدخول غير شرعي لأنظمة الحاسب، وكطريقة لغسيل الأموال.

3– العابثون (vandals): إن فئة العابثين (الذين يتعدون على الملكيات العامة أو الخاصة) أو من الحياة بشكل عام. **ويمكن تقسيمهم إلى مجموعتين** :

أ/ المستخدمون (users) الذين لهم حق استخدام النظام الذي يخترقونه أو يسيئون استخدامه.

ب/ الغرباء (stringers) الذين ليس لهم حق استخدام النظام.

خصائص الجرائم المتصلة بالحاسب

تتميز الجرائم المرتكبة به كأداة أو كهدف للجريمة (وكذلك عبر شبكة الإنترنت) بالخصائص التالية :

1– سرعة التنفيذ : لا يتطلب تنفيذ الجريمة عبر الهاتف الوقت الكثير.

2– التنفيذ عن بعد : لا تتطلب جرائم الحاسب في أغلبها وجود الفاعل في مكان الجريمة.

3– إخفاء الجريمة : جرائم مخفية، إلا أنه يمكن أن تلاحظ آثارها، والتخمين بوقوعها.

4– الجاذبية الإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير التقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات ... إلخ.

5– عابرة للدول (Transnational) : لا تعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، لارتباط العالم بشبكة واحدة.

6– جرائم ناعمة : تمتاز بأنها جرائم ناعمة لا تتطلب عنفاً، نقل بيانات من حاسب إلى آخر.

7– صعوبة إثباتها : تتميز جرائم الإنترنت عن الجرائم التقليدية بأنها صعبة الإثبات.

وهذا راجع إلى الافتقار لوجود الآثار التقليدية للجريمة، وغياب الدليل الفيزيقي (بصمات، تخريب، شواهد مادية). وسهولة محو الدليل. أو تدميره في زمن متناه القصر، يضاف على ذلك نقص خبرة الشرطة والنظام العدلي، وعدم كفاية القوانين القائمة.

8– التلوث الثقافي: لا يتوقف تأثير الجرائم المتصلة بالحاسب عند الأثر المادي الناجم عنها وإنما يتعدى ذالك ليهدد نظام القيم والنظام الأخلاقي في خاصة المجتمعات المحافظة والمغلقة والأمني.

9– عالمية الجريمة والنظام العدلي : نظراً لارتباط المجتمع الدولي إلكترونياً، فقد أصبح مجتمعاً تخيلياً استدعى أن تكون القوانين ذات صبغة عالمية وليست إقليمية كما كان سائداً.

10– التخيلية : أن الومضات والرموز التي ترسل أو التي تخرق وهذه الأوامر الإلكترونية ما هي إلا لنقل معلومات أو أرصدة ولكن بشكل تخيلي يترتب عليها نقل فعلي للثروة والمال والمعلومات.

التعامل مع جرائم الحاسب

تحدث جرائم الحاسب على الرغم من كل الإجراءات الوقائية لمنعها، والحاجة هنا إلى تطوير وسائل وقاية ومهارات في اكتشافها والتحقيق فيها، والحكم على مرتكبيها، ويستخدم (FBI) النموذج التالي في مكافحة جرائم الحاسب.

الوقاية (Prevention)

تشمل تحديد وسائل الوقاية تحليل التهديد والمخاطرة ومعرفة متى تم الدخول إلى أنظمة الحاسب.

وبخاصة:

1- الحماية الفيزيقية.

2- الحماية الشخصية.

3- حماية الاتصالات.

4- حماية نظام التشغيل.

5- التخطيط للتعامل مع الجرائم.

الاكتشاف (Detection) ويشمل إجراءات مثل :

1- إجراءات الاكتشاف.

2- فريق إدارة الأزمة.

3- معالجة ومتابعة الداخلين (المتطفلين).

4- التحقق الداخلي والشرطة.

5- المحاكمة الشفوية.

6- جمع الأدلة.

الحكم (Prosecution) ويشمل إجراءات مثل :

1- قوة الإثباتات.

2- شهادة الخبراء.

3- التقديم في المحكمة.

4- أفعال ما بعد المحكمة.

3- مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية

أولاً- نظام التعاملات الإلكترونية السعودي – تعريف نظام التعاملات الإلكترونية السعودي.

الحاسب الآلي، "التعاملات الإلكترونية أي تبادل أو تراسل أو تعاقد، أو أي إجراء آخر يبرم أو ينفذ – بشكل كلي أو جزئي – بوسيلة إلكترونية "(مادة أولى – 10).

أهداف نظام مكافحة جرائم تقنية المعلومات في المملكة :

ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير إطار نظامي – إزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية. – منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإلكترونية " ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية و الثقافية [1].

ثانياً – سياسة حجب المواقع :

نص قرار مجلس الوزراء القاضي بإدخال خدمة الإنترنت إلى المملكة على حجب المواقع التي تنافي الدين الحنيف والأنظمة الوطنية .[2]

ثالثاً :- الرقابة الذاتية تقويم "للسلوك :

إن ما يمتاز به الإسلام عن غيره أنه يربي مبدأ المراقبة لله تعالى في نفس المسلم.

([1]) موقع هيئة الاتصالات وتقنية المعلومات.

([2]) وحدة خدمات الإنترنت / مدينة الملك عبد العزيز للعلوم والتقنية.

4- المحور الثاني

مواقع التواصل الاجتماعية والشباب – ذكور وإناث

الشباب فئة اجتماعية مهمة في كل مجتمع، لها مميزاتها وخاصيتها، ومنها روح المغامرة والإثارة وحب الاكتشاف والتعرف على الجديد، وهذا جعل الشباب أكثر الفئات الاجتماعية إقبالاً على شبكة الإنترنت.

باعتبارها المجال الرحب للدخول في العالم الافتراضي و الإبحار في كل جهات العالم. يضاف إلى ذلك ما يعيشه الشباب من فراغ في حياته الواقعية، وما يعرفه من مشاكل اجتماعية واقتصادية تحول بينه وبين الاندماج في الحياة وتحقيق الذات. والملاذ من هذه لمشاكل، والمجال الرحب لتحقيق الذات وإثباتها من خلال المشاركة وإبداء الرأي والحوار أو التمكن من التقنيات والإبداع فيها، والتعويض عما يفتقده في محيطه المحلي والواقعي [1].

والشباب ... هم المستهدفون ... لأنهم أمل الأمة ومستقبلها الشباب هم الكنز الإستراتيجي الحقيقي للأمم، وهم الداعم الرئيسي لنهضتها وتقدمها، وهو الوقود الدافع لبناء أمجادها، فبالعناية بهم وبرعايتهم تتقدم الأمم وتنهض، وبعكس ذلك تتأخر وتتقهقر لذا فهم المستهدفون [2].

من منظور اجتماعي :- الركيزة الأولى وأصبحت مواقع التواصل الاجتماعي أهم ما يقصده الشباب على الشبكة العنكبوتية منذ تأسيسها، وأحدثت ثورة وطفرة كبيرة في عالم الاتصال؛ حيث تتيح للفرد أن يتواصل مع أقرانه في كل أنحاء العالم، ولكن ثمة تأثيرات تتركها تلك المواقع في الشباب بعد أن اعتادوا عليها.

تتلخص تلك التأثيرات في الناحية الاجتماعية والإعلامية والدينية، ولتلك المواقع في كل جانب من تلك الجوانب تأثيرات إيجابية وسلبية على مستخدمي تلك المواقع.

يقول الدكتور "أحمد عبد الرؤوف" أستاذ علم الاجتماع بجامعة حلوان: لمواقع التواصل من الناحية الاجتماعية سلبياتها الاجتماعية أكثر من إيجابياتها ويتابع "عبد الرؤوف" : هناك سلبيات أخرى تتعلق بعدم تقبل الرأي الآخر، والنقاشات الحادة، والمشاحنات بين الشباب على تلك المواقع، وهناك أكبر خطر لتلك المواقع، وهو إضاعة الشباب للوقت في التنقل عبر صفحات تلك المواقع، والتحدث في أمور ليس لها قيمة ولا فائدة، وهذا الجانب هو أخطر الجوانب السلبية؛ حيث إن مضيعة الوقت تأتي بالسلب على المجتمع كله وعلى تقدمه، وليس على الشخص فقط.

وأخيراً هذه المواقع أيضاً تؤثر على الجانب الأسري :

حيث يؤدي الدخول عليها إلى العزلة الاجتماعية، وعدم اندماج الفرد مع أسرته، وغيابه عن مشكلات وهموم الأسر وعن المشاركة في المناسبات الاجتماعية، وما إلى ذلك [3].

مواقع التواصل الاجتماعية - / مسميات وخصائص

مواقع التواصل الاجتماعية الإلكترونية (وهي مجموعة من البرامج والمواقع الإلكترونية التي يمكن للمستخدم إنشاء موقع خاص به عليها، أو تحميلها على جهاز هاتفه الذكي أو اللوحي.

يمكنه من خلالها الارتباط والتواصل مع الآخرين برابط القرابة، أو المعرفة، أو الصداقة، أو الاهتمام والهواية، أو زملاء الدراسة والعمل؛ ونحو ذلك من روابط التواصل) كغيرها. حيث تعتبر :-

أ) وعاء بحسب ما يتم ملؤه تكون أي أن العنصر البشري هو الموجه لها والمؤثر أولاً وأخيراً، سلباً أو إيجاباً.

مما ينعكس على الاستفادة منها إيجابياً وسلبياً.

ب) ومن المهم معرفة الإيجابيات للاستفادة منها، ومعرفة السلبيات لتلافيها وعدم الوقوع فيها.

وهذه المواقع والبرامج من خصائصها

أ) الانتشار – انتشرت بشكل كبير وسريع بين المستخدمين ليس على المستوى المحلي والإقليمي بل على مستوى العالم، ولجميع الشرائح حتى الأطفال.

ب) التقريب – مما أدى إلى كسر الحدود الجغرافية، وجعله يبدو كقرية صغيرة تربط أبناءه بعضهم ببعض.

ج) التحلل: عدم التقييد بالأعراف والعادات والتقاليد الاجتماعية عند الغالبية وتتمثل مواقع وبرامج التواصل الاجتماعية في العديد من البرامج والمواقع؛ منها "على سبيل المثال لا الحصر ":

1- البريد الإلكتروني.

---

(1) موقع www.almaaref.org

(2) موقع الاتحاد العالمي لعلماء الإسلام.

(3) باختصار / رابط الموضوع: www.alukah.net/culture

2- المنتديات.

3- المدونات الشخصية.

4- تويتر (Twitter).

5- فيس بوك (Facebook).

6- انستغرام (Instagram) / هو تطبيق مجاني لتبادل الصور وشبكة اجتماعية.

7- تيليجرام (Telegram): هو عبارة عن تطبيق للتراسل الفوري، حر ومفتوح المصدر جزئياً ومتعدد المنصات ويركز على الناحية الأمنية. مستخدمو تلغرام يمكنهم تبادل الرسائل بإمكانية تشفير عالية بما في ذلك الصور والفيديو والوثائق (كافة تنسيقات الملفات المدعومة).

8- يوتيوب (You Tube) ... أفلام وأغاني وغيرها.

9- واتس أب (Whats App). رسائل وصور وفديو

10- فايبر (Viber) :- هو تطبيق يعمل على الهواتف الذكية يتيح للمستخدمين المراسلة الفورية وإجراء مكالمات هاتفية مجانية وإرسال رسائل (نصية، صور، فيديو، صوت).

11- هاي فايف (Hi 5) :- هو موقع ويب وشبكة اجتماعية.

12- بلارك (Plurk) : موقع جديد في عالم التدوينات المصغرة والأحداث وهو موقع Plurk. كلمة Plurk تعني تأريخ الأحداث والمناسبات الخاصة بالشخص.

13- كيك (Keek) : خدمة شبكات اجتماعية مجانية تمكن المستخدمين من تحميل فيديوهات تحديث عن يوميتهم أو الحالة التي يعشونها وتسمى بكيكس.

14- ماي سبيس (Myspace) : موقع يقدم خدمات الشبكات الاجتماعية على الويب تقدم شبكة تفاعلية بين الأصدقاء المسجلين في الخدمة بالإضافة إلى خدمات أخرى كالمدونات ونشر الصور والموسيقى ومقاطع الفيديو والمجموعات البريدية وملفات المواصفات الشخصية للأعضاء المسجلين.

15- بلاك بيري (Black Berry). ويعني (التوت الأسود)، هو نوع من الهواتف الذكية التي تدعم خدمة البريد الإلكتروني.

16- سنابشات (Snapchat) : هو تطبيق رسائل مصورة وضعها إيفان شبيغل وروبرت مورفي، ثم طلبة جامعة ستانفورد، عن طريق التطبيق، يمكن للمستخدمين التقاط الصور، وتسجيل الفيديو، وإضافة نص ورسومات، وإرسالها إلى قائمة التحكم من المتلقين. ومن المعروف أن هذه الصور ومقاطع الفيديو المرسلة على أنها "لقطات" يعيين المستخدمين مهلة زمنية لعرض لقطاتهم من ثانية واحدة إلى 10 ثواني، وبعد ذلك سوف تكون مخفية من الجهاز المستلم وتحذف من الخوادم الخاصة بسناب شات أيضاً [1].

17- لاست أف أم (بالإنجليزية : Lasf. Fm) هي خدمة سماع أغاني مركزها المملكة المتحدة بلغ عدد المسجلين بها 40 مليون من 160 دولة. يستعمل الموقع. كما يقدم الموقع بالإضافة إلى ذلك خدمة الشبكة الاجتماعية [2].

18- غرفة الدردشة (أو غرف المحادثة): في المقام الأول عن طريق وسائل الإعلام لوصف أي شكل من أشكال المقابلات على الإنترنت التي تكون على هيئة مؤتمرات متزامنة (أي التحدث والمناقشة في نفس الوقت) أو تكون أحياناً غير متزامنة (كما في المنتديات) و تستخدم غرف الدردشة في الأساس في تبادل المعلومات النصية مع مجموعة من المستخدمين الآخرين. إتاحة التكنولوجيا الحديثة تقنية تبادل الملفات واستخدام الكاميرا لكي يتمكن الأفراد من روية بعضهم البعض أثناء الدردشة وذلك عن طريق وجود بعض البرامج لتحقيق هذه الأغراض. وقد أتاحه تقريباً (الدردشة عن طريق الإنترنت وخدمة إرسال الرسائل) للمستخدمين أن يرسلو أو يعرضوا صورهم.

مع ارتفاع وافر في نشاط (Sexting)، حيث كان الأفراد يرسلون صور عارية أو صوراً جنسية فاضحة لأنفسهم إلكترونياً لكي ينظر إليها الآخرين، فقد أصبح شائعاً بشكل متزايد في غرف الدردشة. للمستخدمين لتبادل صور عارية أو جنسية. [1] بعض الناس الذين يزورون غرف الدردشة على استخدامها كمكان لتجربة الجنس على الإنترنت، والتي تعرف أيضاً باسم سبرس إكس (cybersex) أو ما يسمى حب على الكمبيوتر في حين لم يكن مادياً قادراً على رؤية زوجاتهم، حيث السيبرانية كانت عبارة عن التحفيز عن طريق القراءة.

في حين أن العديد من وسائل الإعلام في التركيز على هذا الجانب من غرف الدردشة لأنها بالتأكيد يعزز تصنيفاتها، فإن الأمر لا يعني أن هذا الشيء الوحيد التي من أجله يتم استخدام غرف الدردشة في حين أن العديد من الناس يدخلون في "سبرسإكس" لأسباب كثيرة، فمن الصحيح أيضاً أن

---

(1) الموسوعة الحرة

(2) الموسوعة الحرة.

الأشخاص الذين يستخدمون الإنترنت للتعدي الجنسي يستخدمون محادثات سبرسإكس كوسيلة من وسائل التعرف على الضحايا المحتملين الألعاب هي أيضاً كثيرة ما لعبت في غرف الدردشة أمثلة تاريخي هي (initgame) أو (Hunt the Wumpus) على الدردشة [1].

19- وغيرها والمستقبل يخبئ الكثير والكثير من مواقع وبرامج ووسائل التواصل الاجتماعية الأخذة بالانتشار بين المستخدمين؛ بل أصبحت مقصداً شبه أساسي من قبل الجميع صغاراً وكباراً، رجالاً ونساءاً.

من إيجابيات مواقع التواصل الاجتماعية :

* مما ساهم في سرعة انتشارها وكثرة الإقبال عليها ما تتميز به من ميزات وجوانب إيجابية فاعلة، كاستمرار التواصل بين المستخدمين على مدى الأربع والعشرين ساعة، الأمر الذي يزيد في قوة الترابط والعلاقات بينهم، ومعرفة أخبارهم وتوطيد العلاقات من خلال تبادل التهاني بالمناسبات والمواساة عند المصائب والملمات.

*كما أنها تساهم في سرعة تبادل المعلومات، والأخبار، وتكوين الصداقات والتعارف، وتبادل الآراء والأفكار ومعرفة ثقافات الشعوب، والتعرف على كثير من الجوانب الثقافية والاقتصادية والسياسية والسياحية والأدبية واللغوية والعسكرية والدينية وغيرها من المعلومات والصور والمواد المختلفة التي يحتاجون إليها.

*كما أنها مصدر جيد للطلاب في مختلف مراحل التعليم العام والجامعي والعالي، يستخدمون الإنترنت ومواقع التواصل الاجتماعي في إعداد البحوث وإجراء الأبحاث والدراسات التي تساهم في رفع مستوى تحصيلهم العلمي، ومعدلهم الدراسي.

* إضافة إلى أنها بوابة للبحث عن فرص عمل وتوظيف؛ حيث يستخدمها الشباب في البحث عن فرص عمل، كما تقوم الشركات بالتسويق والإعلان عما يتوفر لديها من فرص عمل، والتسويق لمنتجاتها ، وفي الدعاية والإعلان ؛ بل أنها صارت بوابة للتسويق التجاري ومصدر من مصادر الدخل السريع.

*كما أن لهذه المواقع دور فاعل في تفعيل الأعمال التطوعية والاجتماعية المفيدة للمجتمع بيسر وسهولة.

*كما أن مواقع التواصل هي نافذة إيجابية في جعلها وسيلة لنشر التوعية الصحية والمرورية والأمنية والاجتماعية، لتساهم في مساعدة المختصين في نشر وتوعية أفراد المجتمع بما يفيدهم في عموم المجالات وبطريقة سهلة وسلسلة يكون لمستخدمين تلك المواقع القابلية لها.

* ساهمت في تحقيق الكثير من الجوانب الإيجابية في مجالات الطب والصناعة وإدارة الشركات والأعمال والأموال والمنشآت العملاقة، وعقد الاجتماعات والتواصل بين جميع الأطراف من أي مكان بالعالم.

*كما أنها وسيلة فاعلة في إجراء الاستفتاءات وقياس ومعرفة آراء الناس والتصويت على كثير من الجوانب. وغير ذلك من المجالات الإيجابية لهذه التقنية التي تمثل أحد أهم الثورات الحديثة في عالم الاتصال، والتي تتيح للجميع أن يتواصلوا فيما بينهم بكل يسر وسهولة.

ويمكن اختصار ذلك بأن برامج ومواقع التواصل الاجتماعية في الجملة؛ ذات قيمة ومنفعة ومردود إيجابي على الفرد والمجتمع والعالم، بشرط أن نحسن استخدامها، وأن نسخرها لكل ما هو جميل وإيجابي في حياتنا لتكون الفائدة المرجوة منها مواقع التواصل الاجتماعية :- بحسب استخدامنا لها فإذا مخالفاً لما هي له، وبشكل سلبي وعشوائي، فهذا لا شك أنه سوف يترتب عليه العديد من الجوانب السلبية، بل وقد تكون كارثية ومهلكة للفرد والمجتمع بأسره.

ومن صور الاستخدام السلبي لها "على سبيل المثال لا الحصر ".

مواقع التواصل والتأثيرات النفسية

* أنها أصبحت ميداناً خصباً لتداول الإشاعات والأخبار المكذوبة والمغلوطة، التي تفتقد لأبسط أبجديات المصداقية، ناهيك عن التأكد من المصدر أو حتى ذكره، حتى صارت مرتعاً للمغرضين وأصحاب الشبه والأوهام الفكرية والعقدية والأدبية والأخلاقية والسياسية، من خلال نشرهم مواد ضارة ومشككة في الحقائق ومثيرة للفتنة والريبة، تؤدي إلى قلق المستخدم والمجتمع والوطن ونجد أن الشائعات الشائعة يطلقها الجبناء، ويصدقها الأغبياء الذين لا يستخدمون عقولهم ويستفيد منها الأذكياء.

الشائعات كم دمرت من مجتمعات وهدمت من أسر، وفرقت بين أحبة الشائعات كم أهدرت من أموال، و ضيعت من أوقات ولها أنواع الشائعات منها الشائعة الزاحفة الشائعة الغاطسة: الشائعة الأمل : شائعة الخوف: شائعة الخيانة: شائعة البعبع الشائعة العنصرية (التمييزية) التي تحمل موقفاً ما من جماعة عرقية أو طائفية [2].

* ومن محاسن وجود المتكلم الرسمي لكثير من المصالح والدوائر هو القضاء على الشائعة في مهدها حيث يتم البيان والتوضيح إعلامياً وبشكل سريع.

* ظاهر التحرر برزت ظاهرة خطيرة بين بعض الشباب؛ وهي تفاخرهم بالإلحاد "وهم جزما لا يعنون الإلحاد بمعناه ومفهومه، وإنما يقصدون التحرر من الأحكام الشرعية" في كتاباتهم وتغريداتهم.

---

(1) الموسوعة الحرة.

(2) موقع صيد الفوائد باختصار.

مواقع التواصل وتأثيرها على اللغة العربية والثقافة العامة.

كما ظهر فيها لغة جديدة بقصد الاختصار وإظهار المستوى الثقافي من خلال إدخال بعض الكلمات والألفاظ غير العربية للعربية ودمجها لتكون لغة تخاطب ومصطلحات بين المستخدمين. واللغة العربية من الثوابت والخطوط الحمراء لأنها لغة القرآن دستور الأمة.

مواقع التواصل والانحدار التربوي : كما أن هناك سلبيات تتعلق بالتنصل من أدب الحوار والنقاش وتقبل الرأي الآخر.

كما أوجد طبقة دونية من المجتمع :– هي حثالة المجتمع "خاصة من يتخفون وراء أسماء وهمية.

ومن سلبياتها التربوية والغير أخلاقية :– في غياب عين الرقيب. حقيقة أرى أنه كما يقول المثل الشق أوسع من الرقعة لأن الهجمة شرسة ومن كل اتجاه وصوب وعلى مدار الساعة ولها مغريات وسهولة الوصول لها .. إلخ.

ومن السلبيات خدش الحياء والأدب :– بكسره وزوال حاجز الحياء خصوصاً بين الشباب والفتيات مراهقين ومراهقات بل أصبحت ظاهرة في مواقع التواصل من خلال التتابع والردود والمراسلات الخادشة للحياء والوقوع في المحظورات الشرعية بكل حرية ودون أي خجل أو أدب أو حياء من أي أحد؛ بل أن ما عرف بقضايا الابتزاز وكذلك التحرش والاغتصاب كان لتلك المواقع دور فاعل فيها [1].

مواقع التواصل من منظور صحي

بل أنه نشأ داء عصري جديد، عرف "بدأ إدمان الإنترنت خاصة من قبل الأطفال والنشء الذين أقبلوا على تلك التقنية بشكل مفرط ودون رعاية أو متابعة من ذويهم؛ حتى أدمنوا الجلوس إليها للساعات الطويلة؛ مما أنعكس عليهم سلباً على حياتهم وصحتهم ومستوى تفكيرهم وعلاقاتهم الاجتماعية والأسرية. ومن سلبياتها ومن سلبياتها أنها خلقت بيئة حاضنة للأمراض النفسية والانطواء على الذات، أو بين أفراد معينين.

عندما يعتاد الشخص على استعمال هذه الشبكات يصاب بالإدمان و بالتالي في وقت لاحق "بأمراض نفسيه عصرية " /: قلق، وعدم استقرار، حيرة، عصبية وغيرها [2].

سلبيات الواتس أب (Whats App) والإنستغرام (Instagram) على الأسرة والمجتمع: خصائصها وتأثيراتها الأسرية

لعل من أخطر برامج مواقع التواصل الاجتماعي سلباً على الأسرة والمجتمع هو برنامج الواتس أب (Whats App) والإنستغرام (Instagram).

إذ أن الكثير من المشاكل الأسرية؛ منها ما أداء إلى القطيعة حصلت بسببهما، وهذا لما لدى البعض من حساسية مفرطة إتجاه الآخرين والتواصل معهم.

ومن مشاكل الواتس أب (Whats App):

هو تطبيق تراسل فوري، محتكر، ومتعدد المنصات للهواتف الذكية. ويمكن بالإضافة إلى الرسائل الأساسية للمستخدمين، إرسال الصور، تناقل الرسائل والمعلومات والأخبار دون تثبت، مما روج للإشاعات.

أما مشاكل الإنستغرام (Instagram):

الإنستغرام ليس مجرد موقع للتواصل من خلال الصور والمقاطع؛ بل هو مشروع تجاري واستثماري من خلال عرض المنتجات والتسويق لها والتعريف بها؛ إلا أن سوء استخدامه جعل منه جزء من مشاكل مواقع التواصل إن لم يكن هو أخطرها على الأسرة بوجه التحديد.

ففي السابق كانت أحوال الناس غير معلومة؛ بل سرية حتى عن أقرب الناس لهم، أما اليوم فكل حركاتهم وسكناتهم فهي معروفة وعلنية؛ فكل فرد من أفراد الأسرة يصور ويرسل مباشرة عبر حسابه، ليباهي الغير فيما هو عليه من حال، حتى صار الناس في حال يرثى فيها لما يترتب على تلك الإضافات من مشاكل وخلافات تنشأ جراء تلك المباهات والتسابق في نشر الصور.

فهي "من وجهة نظري الخاصة – الكلام –كاتب المدونة" أنها أخطر المشاكل خاصة على الأسرة – **وذلك من عدة جوانب** :

يحرص على عرض صورة الخاصة به، والتي تمثل الرحلات والزيارات والمناسبات الخاصة به أو التي حضرها، أو الأحداث التي تقع أمامه أو لبعض الأقارب والأصدقاء والزملاء والمعارف.

وقد تكون تلك الصور المضافة غير مناسبة من قبل وجهة نظر أنها انتهاك لخصوصية الغير.

أو الأعظم من ذلك الغيرة والتنافس بين الأسر خاصة في المناسبات والسفر والرحلات، اللجوء للكذب والنفاق [3].

أجهزة التواصل الاجتماعي من منظور شرعي

إن وسائل التواصل الاجتماعي كشفت ما في المجتمعات من خلل في التدين، وضعف في التربية، وانحطاط في الأخلاق.

---

[1] موقع المسلم

[2] باختصار موقع / www.almaaref.org

[3] منشوره على الشبكة – أبو عبد العزيز – بتصرف

الحياء وهذه الغفلة قضت على كثير منها وسائل التواصل الاجتماعي، فصار الكلام الفاحش البذيء يتناقله كثير من الشباب والفتيات، بل ربما الأطفال، ناهيكم عن الصور الفاضحة، والمقاطع الفاحشة، والتباهي بانتهاك الحرمات، والمجاهرة بالسوء، فيحكي بعضهم ما عمل البارحة من فواحش وقد بات يستره ربه سبحانه، فيصبح يكشف ستر الله تعالى عليه على الملأ من الناس، بل على ألوف وملايين، وهذا مجاهرة بالإثم، ولو كان كاذباً فيما قال، ولو تخفى خلف أسماء وهمية؛ فإنه لن يخرج من دائرة المجاهرين الذين لا يعافون، ومن يشيعون الفاحشة في الناس – وأخطر من ذلك أن هذه الوسائل فتحت عيون من فيهم ضعف على أنواع من الفواحش.

– ومن الآثار الخبيثة لها أنها جرأت الفساق والفاسقات على الشرع الحكيم بالخوض فيه بلا علم، ورد النصوص أو تأويلها، وتهوين الواجبات والمحرمات، وبث الشبهات لإسقاط كثير من الأحكام.

– وأخطر من ذلك أن الزنادقة والملحدين استغلوا وسائل التواصل الاجتماعي لكسر المقدسات في نفوس المسلمين، وتهوينها في قلوبهم بالتسمي بأسماء الله تعالى، أو الاتصاف بأوصافه سبحانه، أو السخرية به عز وجل، أو الطعن في رسلة وكتبه وشرائعه إن وسائل التواصل الاجتماعي أوعية لتخزين الخير أو الشر ونشرهما [1].

مواقع التواصل الاجتماعي والأبعاد الأمنية :

ومن السلبيات الأمنية :

أنظمة الذكاء الاصطناعي: مع بدايات الإنترنت كان إذا ما بحث الجميع في محرك البحث ظهرت نفس النتائج دون اختلافات بين الأفراد. أما اليوم فقد اختلف الوضع إذ أصبحت تتحكم في الإنترنت (أنظمة الذكاء الاصطناعي) والتي تدرس وتحلل شخصية كل منا وبناء عليه يتم تحديد النتائج التي يجب أن تظهر عند البحث بالمفردات المختلفة، أن أنظمة الذكاء الاصطناعي سوف تقرر ما الذي يجب أن تراه وما لا تراه ! ما هي الآراء التي يستحب أن تقرأها وآراء الاتجاه المعاكس التي لا يجب أن تعرف عنها شيئاً.

والصين على سبيل المثال حظرت تويتر ودعمت موقعاً صينياً مشابهاً يسمى (رينرين renren) [2].

– ووسيلة تجنيد الجماعات الإرهابية للشباب : حذر باحثون ومتخصصون في الشأن الفكري من خطورة شبكة الإنترنت وتنامي آثارها السلبية على الأمن الفكري من خلال إمكانية تنبي أفكار منحرفة تؤدي إلى زعزعة العقائد والإساءة إلى الدين وكذلك آثارها الخطيرة عبر إمكانية تجنيد الشباب لدى الجماعات الإرهابية اقتناعهم بالفكر التكفيري أو استقطابهم تجاه المنظمات الماسونية وغيرها [3].

من الطرق لحماية الشباب من وسائل التغرير التي تستهدفهم وتستهدف استقطابهم :-

تحصين الشباب :– وعن أفضل الطرق لحماية الشباب من وسائل التغرير التي تستهدفهم وتستهدف استقطابهم، أجاب "د. التويجري"، قائلاً: "من المهم كشف الحقائق أمامهم مما يجري على الساحة في نطاق الأحداث الدامية التي ترتكب؛ نتيجة صراعات القتل والذبح العشوائي بين تلك التنظيمات، وإشعارهم بأن مسؤوليتهم الأولى هي حماية وطنهم ومجتمعهم والالتفاف حول قيادتهم "، مؤكداً على ضرورة حماية الرموز من تشويه شبكات التواصل الاجتماعي حتى لا يتم نسف المرجعية الصادقة وإفراغ الساحة للمتصيدين داعياً إلى ضرورة شغل الفراغ لدى الشباب بالأشياء النافعة والمفيدة.

جمعيات تطوعية :– وقال الأستاذ " خالد بن عبد العزيز اليحيا " – مستشار قانوني – إن الواجب علينا أن نعمل على تكوين جمعيات مجتمع مدني تطوعيه تستطيع أن تشغل أوقات الشباب وتنمي مهاراتهم ومعرفتهم وتشبع ذواتهم، بحيث لا ينغمسون في أفكار متطرفة، مثل جمعيات البيئة وجمعيات الهوايات وجمعيات تطوعية لتنظيم المرور.

انخفاض تقدير الذات :– وأضاف أن أكبر ما يدمر شبابنا هو انخفاض تقدير الذات لديهم؛ فكلما انخفض تقدير الذات لدى الشاب كلما انزلق في أعمال غلو وتطرف ومحاولة لإظهار الذات بأي وسيلة؛ فلذلك يجب أن يكون موضوع إشراك الشباب بالنهوض بوطننا هو مشروع وطني كبير كل يجود به بما يستطيع، سواء من رجال الأعمال أو من أصحاب الخبرة أو من الجمعيات والغرف التجارية، وكل مؤسسات المجتمع المدني والدولة.

مشاكل الشباب :– أن من أهم المشاكل الرئيسة التي تواجه شبابنا وتعيقهم عن العمل وكسب السوق هو أن بعض الوزارات والمؤسسات المعنية بالعمل تسن أنظمة من شأنها غلق نوافذ وفرص العمل على الشباب، من خلال التعقيدات والمتطلبات الإجرائية، ومن خلال أيضاً جعل بيئة عمل المؤسسات الصغيرة والمتوسطة بيئة صعبة جداً تعرض من فيها إلى الخسارة والخروج من السوق؛ توفير العمل :– إن مسؤولياتنا جماعية لتوفير الفرص لهم وإعادتهم إلى

---

(1) موقع الشيخ / د. إبراهيم بن محمد الحقيل / مقتطفات من خطبة بعنوان أجهزة التواصل الاجتماعي نهر بر وخير في بحر اثم وشر –/ http://www.alukah.net/sharia/

(2) العدد 17217 الرياض – باختصار.

(3) ملتقى الأمن الفكري بجامعة نايف / الرياض عدد 16563 باختصار.

الخطيرة وإعداد ترتيبات جيدة لهم في حياتهم، وإشعارهم أن المستقبل أمامهم ونشعرهم بقيمتهم الذاتية وقيمتهم في مجتمعهم وليس عبر أنظمة وإجراءات تزيد من إحباطهم وابتعادهم عن واقعهم ووضعهم.

حرية التعبير : وعن دور التنشئة، من المؤسف أننا لم نترك لأبنائنا هوامش جيدة من بناء القيمة الذاتية وحرية التعبير عن مشاعرهم وآرائهم وقيمة الحوار في حياتهم وأهمية الاختلاف وليس الخلاف، لكننا أنشأنا شبابنا منذ الصغر على حسم الأمور في قضية الحلال والحرام والخطأ والصواب، ومن هنا يجب أن نوضح لهم أن الحياة لهم مشارب مختلفة وأن الله خلق الناس بهذه الكيفية لحكمة يعلمها، ويجب أن نتفهم طبيعة الاختلاف بين البشر لا أن ننكرها عليهم ".[1]

الإرهاب المعلوماتي [2]

بعد التطور الهائل في تقنية المعلومات ونظماً لاتصالات وغيرها انتشر مفهوم الإرهاب المعلوماتي (ارهبيوا المعلومات) واتسع مجال هذا المفهوم ليشمل مجالات عديدة لم يتطرق لها الفكر من قبل ومن المخاطر التي لا يستهان بها في استخدام الإرهاب المعلوماتي عندما يتم اختراق نظم المعلومات عبر الشبكة وذلك لما فيها من تحديد الخصوصية للمعلومة سواء كانت هذه المعلومة سياسية، أو عسكرية، أو اقتصادية، أو أمنية أو خلافها. وأصبح الإرهابيون يعرفون تمام المعرفة البيئة المعلوماتية للمراكز المستهدفة.

وكذلك نظم تدفق وانتشار المعلومات في المعدات وشبكات الاتصال والموقف التفصيلي لبرامج إرهاب.

المعلومات :

* يسبب شللاً تاماً في أنظمة القيادة والسيطرة والاتصالات المدنية والعسكرية الأرضية والفضائية.

تعطيل المعدات الإليكترونية لكافة الأنظمة. أو اختراق النظم المصرفية.

* أو ارباك حركة الطيران أو شل محطات الطاقة.

* وهذا يعني تفوق الهجمات الإرهابية في تأثيرها الصراعات المباشرة المسلحة فإرهاب الغد يفوق دماره وتأثيراته العديد من القنابل الذرية بواسطة لوحة مفاتيح من على بعد آلاف الكيلومترات.

* وهؤلاء متحفظون وعملياتهم سرية ويضللون عند البدء لتكون ضربتهم التالية قاضية ومنهية.

مجالات نشاط الإرهاب المعلوماتي

* ينفذ الإرهاب المعلوماتي بواسطة جماعات منظمة قد تكون محلية أو إقليمية أو دولية.

* أو قد يكونوا من الهواة (الهكرز) وهؤلاء عادة همهم السرقة أو نشر المعلومات وليس التدمير وتزوير المعلومات وكلاهما يسبب ضرراً.

جرائم الإرهاب المعلوماتي

وتهدف جرائم الإرهاب المعلوماتي الأضرار بالمعلومات والبرامج والاتصالات في القطاعين العسكري والمدني وتنحصر جرائم الإرهاب المعلوماتي في عمليات الاختراق الحاجز الأمني لنظم المعلومات وكذلك الخلل الذي يصيب الحاسوب وفق الأساليب التالية :-

صناعة ونشر الفيروسات / بغرض الأضرار بنظم الحاسوب والمعلومات المخزنة.

الدخول الغير مصرح / لأنظمة والمعلومات (الاختراقات).

تعطيل وشلل أجهزة الحاسوب – دون اختراق عن طريق إرسال عدة رسائل ملغمة.

انتحال الشخصية – لإخفاء هويته أو الاستفادة من مكانة الضحية وتعتبر انتحال الشخصية من أكبر سلبيات الإنترنت الأمنية.

المضايقة والملاحقة – في التحكم في الضحية في / ابتزاز، و تخويف، أو تهديد

التغرير والاستدراج وهنا تتعدد الأساليب والطرق بحسب الغاية.

التشهير وتشويه السمعة – بنشر معلومات (سرية أو مضللة أو مغلوطة) ضد فرد، أو جماعة أو مؤسسة أو شركة ... إلخ.

صناعة ونشر الإباحية – بعرض صور جنسية ومواد حيه لنساء ووسائل اتصال ... إلخ.

النصب والاختيال تعتبر مجال رحباً في عدد مجالات.

5- المحور الثالث

([1]) / الرياض/ العدد 16865 – تحقيق وتقارير مسئولية المجتمع أن يتجاوز أخطاءه ويمضي مع أبنائه إلى الأمام بوعي وبلا تردد – باختصار.

([2]) مقتطفات من ندوة المجتمع والأمن دوره (5) كلية الملك فهد الأمنية بالرياض – الجرائم اليكترونية الملامح والأبعاد – 5/ 7/ ربيع الثاني / 1428 هـ الموافق 22 – 24/ أبريل 2007 م.

علم الأدلة الرقمية والتحقيق في جرائم المعلومات

علم الأدلة الرقمية والتحقيق في جرائم المعلومات بحيث تغطي معظم الطرق العملية المحتملة للتعامل مع تلك الأدلة وطرق استخراجها وتحليلها في وقت انتشرت فيه التقنية الرقمية في التعاملات اليومية وازدادت استخدامات الحاسبات والإنترنت وجرائم الإنترنت وبناء على هذه التطورات المهمة في مجال التقنية جاءت أهمية علم التحقيق في الأدلة الرقمية، من خلال التطبيق العملي في استخدام الدليل الرقمي والهواتف الذكية وفحص وتفسير النتائج، والإلمام بالمعايير القياسية للتعامل مع الأدلة الرقمية باستخدام تطبيقات متخصصة بما يضمن حجيتها في الإثبات القانوني أمام الجهات القضائية [1].

تعريف علم التحقيق في الأدلة الرقمية :

جميع الإجراءات الخاصة بالمضبوطات الرقمية ذات العلاقة بالجريمة بالمحافظة عليها ونقلها وفحصها وتحليلها وكتابة التقارير لإثبات أو نفي أو الاستدلال على حالة جنائية لخدمة التحقيق الجنائي والبعض يسميه التحقيق الجنائي الرقمي.

أنواع الأدلة الرقمية

1- تسجيل مراقبة /

2- منظم أو حافظ بيانات

3- أداة اتصال

خصائص التحقيق في الأدلة الرقمية

* الأدلة (قد تكون نتيجة تكامل بيانات عدة أجهزة أو وسائط). (لا تتواجد بالضرورة في بمسرح الجريمة.

* يجب أن يعالجها عناصر وطنية (السرية والخصوصية). والأدلة الرقمية يصعب التخلص منها بسهولة.

* بيانات الأدلة يمكن أن تتغير بسهولة عمداً أو عفوياً. بيانات ضخمة وغير مشاهدة.

علم التحقيق في الأدلة الرقمية

أن علم الأدلة الرقمية والتحقيق في جرائم المعلومات، علم جديد حيث التعامل مع تلك الأدلة وطرق استخراجها وتحليلها، تتطلب اكتساب الخبرات في مختلف تقنيات التحقيق الجنائي الرقمي، والإلمام بالمعايير القياسية للتعامل مع الأدلة باستخدام تطبيقات متخصصة بما يضمن حجيتها في الإثبات القانوني أمام الجهات القضائية وحيث أن هذا العلم متطور ومتجدد بشكل سريع ويتطلب من العاملين مواكبة هذا التغير والتطور السريع، ليتحقق الأهداف أولاً – مثل :-

* التعرف على المعايير القياسية للتعامل مع الأدلة الرقمية وكيفية التحفظ على الأدلة الرقمية.

* استخراج الأدلة الرقمية من ملفات نظم التشغيل وملفات المستخدمين.

* تحليل الجرائم باستخدام تطبيقات التحقيق الجنائي الرقمي.

* التعامل مع البيانات المخفية وتتبع الجناة عبر الإنترنت.

* التعرف على الثغرات الأمنية في نظم المعلومات.

ثانياً :- لكي يواجه التحديات العديدة منها :-

أولاً – التحديات العامة

1- يقود هذا التخصص شركات القطاع الخاص وليس الحكومات.

2- معظم خبراء الأدلة الرقمية (مهتمين أكثر من أنهم متخصصين).

3- الأدلة الرقمية لازالت في مرحلة مبكرة من النضج.

4- يختلف علم التحقيق الرقمي عن علم الأدلة الجنائية الأخرى (البصمات والبصمة الوراثية) في طرق الفحص والأدوات وأهمية النتائج والخصوصية ... إلخ.

5- لا يوجد معايير قياسية مطبقة للمتعاملين مع الأدلة الرقمية حتى الآن.

6- يتعامل مع مجتمع العدالة والتقنية وعلم التحقيق الجنائي وتختلف متطلبات هذه المجتمعات.

ثانياً – التحديات التقنية في المعامل الأدلة الرقمية :

---

(1) الصحيفة الاليكترونية

1- تزايد كبير في حجم البيانات المشفرة وطرق إخفاء البيانات.

2- زيادة في حجم استخدامات التقنية والاعتماد عليها.

3- زيادة في حجم البيانات وسعة وسائط التخزين.

4- إعادة بناء الأحداث الرقمية يعتمد على فرضيات متعددة.

5- العديد من منصات أنظمة التشغيل وأنظمة الملفات وتحتاج خبرات مختلفة.

6- سعات تخزين البيانات عالية ومتزايدة (SANs Terabytes)، وأسعارها في انخفاض.

7- بيانات المستخدمين متراكمة من سنوات والتحقيق في الأدلة الرقمية على الحوسبة السحابية والدعاوي القضائية المرتبطة بها أصبحت مكلفة جداً.

8- الحوسبة السحابية من يملك البيانات فعلياً في بيئة الحوسبة.

الحوسبة السحابية : (Cloud computing) هي مصطلح يشير إلى المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع توفير عدد من الخدمات الحاسوبية المتكاملة دون التقيد بالموارد المحلية بهدف التيسير على المستخدم، وتشمل تلك الموارد مساحة لتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية، كما تشمل قدرات معالجة برمجية وجدولة للمهام ودفع البريد الإلكتروني والطباعة عن بعد، ويستطيع المستخدم عند اتصاله بالشبكة التحكم في هذه الموارد عن طريق واجهة برمجية بسيطة تبسط وتتجاهل الكثير من التفاصيل والعمليات الداخلية.

إجراءات الادعاء

1- وقت محدد. 2- جودة النتائج 3- الفحص الفني

ثالثاً – تحديات الموارد البشرية.

* التدريب يرتبط بمنتجات تقنية مختلفة ومتجددة وأجور خبراء التقنية (الوطنية) غير مدعومة.

* الخبرات على المنتجات القديمة أيضاً مطلوبة.

* ندرة المتخصصين وتكاليف التدريب مرتفعة ومخرجات الجامعات المحلية لا تخدم.

* عمل أمني وتقني في نفس الوقت، محاذير الاستعانة بالخبرات الأجنبية في التحقيق.

رابعاً – التحديات التكوينية لعلم التحقيق في الأدلة الرقمية.

(علم الأدلة الرقمية) – خليط من ثلاث مجتمعات معرفية

1- التحقيق الجنائي : هي علوم تطبيقية تنطوي على دراسة الحقائق، وتستخدم للتحقق من وجود جريمة وإثبات ذنب المجرم، التحقيق الجنائي الكامل يمكن أن يشتمل البحث والمقابلة والاستجواب وجمع الأدلة وحفظها وعدة أساليب مختلفة للتحقيق [1]، التحقيقات الجنائية في العصر الحديث تستخدم عادة عدة تقنيات علمية حديثة تعرف بالعلم الشرعي.

2- علم الحاسوب أو المعلوماتية: يدرس الحوسبة ومعالجة البيانات والنظريات والتطبيقات التي تشكل الأساس لأتمته نقل المعلومات وتشغيلها وتحويلها، وذلك بدراسة برمجيات الحاسوب عتاد الحاسوب بشكل علمي مجرد في بعض الدول العربية يطلق على مصطلح علم الحاسب الآلي المعلوماتية اختصاراً وليس بقصد خلطة مع العلوم الأخرى وخاصة التخصصات المتعلقة بتكنولوجيا المعلومات المهتمة بالتطبيق غير المبني على أسس علمية [1].

3- النظم العدلية والتشريعات : ما يتعلق بالمحاكم والمرافعات وقوتها (الأدلة الرقمية) ... إلخ.

* معايير قبول (الأدلة الرقمية، خبراء الأدلة)

* ما هو معدل احتمالية الخطأ في الإجراءات المنفذة (نقص في الخبراء).

* تعريف دقيق للجريمة الإلكترونية بمنظور الشريعة الإسلامية.

* عقبات في تبادل المعلومات بين المحققين والادعاء.

* جريمة دولية وعقبات في اتفاقيات تسليم المجرمين بين الدول.

مسرح الجريمة في الجريمة الإلكترونية كما سبق وبينا أن من خصائص أنها عابرة للقارات أيمكن يكون الجاني في مدينة والمجني عليه في أخرى أو دولة أخرى أو قارة أخرى.

تكمن أهمية علم التحقيق في الأدلة الرقمية للأسباب التالية :-

1- جرائم التقنية خطيرة جداً ومكلفة. 2) السرعة في التنفيذ.

---

(1) الموسوعة الحرة

3) جريمة دولية. 4) صعوبة الإثبات والإدعاء (عدم وجود الأعداء 3 المحددين)
5) أنها في تزايد مستمر. 6) أنها تتم بسرية خاصة (ناعمة) لا تستخدم العنف الظاهر.
7) لا يبلغ عنها عادة.

أنواع الأدلة الرقمية :

(هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون) والذي يلاحظ على هذا التعريف أنه يقصر مفهوم الدليل الرقمي على ذلك الذي يتم استخراجه من الحاسب الآلي ... * / أرشيف قانونيه.

خصائص الدليل الرقمي :

يعتبر الدليل الرقمي دليلاً غير ملموس أي هو ليس دليلاً مادياً، فهو – أي الدليل الرقمي – تلك المجالات المغناطيسية أو الكهربائية، ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عملية نقل لتلك المجالات عن طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة.

يعتبر الدليل الرقمي من قبيل الأدلة الفنية أو العلمية، وهو من طائفة ما يعرف بالأدلة المستمدة في الآلة.

إن فهم مضمون الدليل الرقمي يعتمد على استخدام أجهزة خاصة بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن اعتباره دليلاً رقمياً، وذلك لعدم إمكانية الاستدلال به على معلومة معينة، ما يعدم قيمته التدليلية في إثبات الجريمة ونسبها إلى الجاني.

مميزات الدليل الرقمي :- يتميز الدليل الرقمي بعده مميزات أهمها.

1- يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل.

2- إن محاولة الجاني محو الدليل الرقمي بذاتها تسجل عليه كدليل، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده.

3- إن الطبيعة الفنية للدليل الرقمي تمكن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف كما سنرى لاحقاً.

أنواع الدليل الرقمي ومجاله في الإثبات الجنائي – أولاً – أنواع الدليل الرقمي وأشكاله :

إن التعريف بالدليل الرقمي يحتم علينا تحديد أنواعه و أشكاله حتى يتسنى فهم الهيأة التي يتخذها للحكم على قيمته القانونية فيما بعد، ولذ سنتناول أولاً أنواعه ثم نحدد الأشكال التي يبدو عليها هذا الدليل وذلك على النحو التالي :

1- أنواع الدليل الرقمي : يمكن تقسيم الدليل الرقمي لنوعين رئيسين:

أ- أدلة أعدت لتكون وسيلة إثبات :

وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي :

1- السجلات التي تم إنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

2- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة وتتم معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.

ب- أدلة لم تعد لتكون وسيلة إثبات :

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهي ما يمكن تسميه أيضاً بالآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية.

والواقع أن هذا النوع من الأدلة لم يعد أساساً للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي تجري عبر الإنترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك.

وتبدو أهمية التمييز بين هذين النوعين فيما يلي :

1- النوع الثاني من الأدلة الرقمية هو الأكثر أهمية من النوع الأول لكونه لم يعد أصلاً ليكون أثراً لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

2- يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه لكونه قد أعد أصلاً لأن يكون دليلاً على الوقائع التي يتضمنها، في حين يكون الحصول على النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

3- أن النوع الأول قد أعد كوسيلة إثبات لبعض الوقائع فإنه عادة ما يعمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل من إمكانية فقدانه، وعلى عكس النوع الثاني حيث لم يعد ليحفظ ما يجعله عرض للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلاً.

2- أشكال الدليل الرقمي: يتخذ الدليل الرقمي ثلاثة أشكال رئيسه هي:

* الصور الرقمية / التسجيلات.

* النصوص المكتوبة [1].

تسجيل / مراقبة. 2 منظم / أو حافظ بيانات 3- تسجيل / مراقبة

الإجراء / بعد الاعتداء / القبض

الاستجابة للأحداث

التحريز وحماية الأدلة

نقل الأدلة 4) فحص البيانات

تحليل النتائج 6) التقارير 7) الاستجواب

نطاق العمل بالدليل الرقمي:

إن الاهتمام الذي يحظى به الدليل الرقمي قياساً بغيره من الأدلة الأخرى المستمدة من الآلة مرده انتشار استخدام تقنية المعلومات الرقمية، والتي تعاظم دورها مع دخول الإنترنت شتى مجالات الحياة، وأصبح بذلك هذا الوسط مرتعاً لطائفة من الجناة يطلق عليهم اسم المجرمين المعلوماتيين، فالجرائم التي يرتكبها هؤلاء تقع في الوسط الافتراضي أو ما يمكن تسميته بالعالم الرقمي، ولذا كان الدليل الرقمي هو الدليل الأفضل لإثبات هذا النوع من الجرائم، لأنه من طبيعة الوسط الذي ارتكبت فيه، ومن هنا بدت أهمية هذا النوع من الأدلة، ولكن أيعني ذلك أن الدليل الرقمي ينحصر مجاله كدليل إثبات فقط على جرائم المعلوماتية ؟

- يجب التنويه إلى أنه لا تلازم بين نطاق العمل بالدليل الرقمي ومشكلة إثبات الجريمة المعلوماتية، فمن ناحية فإن الدليل الرقمي مثلما يصلح لإثبات الجريمة المعلوماتية ويعتبر في ذات الوقت الدليل الأفضل لإثباتها، فإنه من ناحية أخرى يصلح لإثبات الجرائم التقليدية إن جاز التعبير، حيث يميز الفقه في هذا الشأن بين نوعين من الجرائم :

أ- الجرائم المرتكبة بواسطة الآلة : وهذا النوع من الجرائم يستخدم فيه الحاسب الآلي والإنترنت كوسيلة مساعدة لارتكاب الجريمة، مثل استخدامه في الغش أو الاحتيال أو غسل الأموال أو لتهريب المخدرات، وهذا النوع من الجرائم لا صلة له بالوسط الافتراضي إلا من حيث الوسيلة، وبكلمة أوضح فإن الجريمة في هذه الحالة هي جريمة تقليدية استعملت في ارتكابها أداة رقمية، فبرغم عدم اتصال هذه الجريمة بالنظام المعلوماتي فإن الدليل الرقمي يصلح كدليل لإثباتها.

ب- جرائم الإنترنت والآلة الرقمية : وهذا النوع من الجرائم يكون محله جهاز الحاسب الآلي أو الآلة بصفة عامة، بحيث يكون الاعتداء واقعاً إما على الكيان المادي للآلة، وهذه يمكن اعتبارها جريمة تقليدية تلحق النوع الأول، وإما يكون الاعتداء واقعاً على الكيان المعنوي للحاسب أو الآلة أو على قاعدة البيانات أو المعلومات التي قد تكون على شبكة المعلومات العالمية، مثال انتهاك الملكية الفكرية، وجرائم القرصنة وغيرها، وهذا النوع من الجرائم هو ما يمكن تسميته بجرائم المعلوماتية والتي يكون الدليل الرقمي هو الدليل الأفضل لإثباتها إن وجد.

دورة إجراءات الأدلة

1- تحديد الحدث الجنائي. 2- حماية مسرح الجريمة ...

3- استخراج الأدلة. 4- جمع الأدلة ....

5- تحليل البيانات ... 6- الاستجواب (التحقيق، الادعاء).

خبراء الأدلة الرقمية ؟

[1] أرشيف قانونية / منتديات ستار تايمز – الدليل الرقمي في مجال الإثبات الجنائي / أ. طارق محمد الجملي عضو هيأة التدريس بكلية القانون – جامعة قاريونس.

خبراء الأدلة الرقمية عناصر هامة في العمل الأمني ويخدمون عدة مستفيدين والحاجة لدعم خبراء الأدلة الرقمية (الوطنية) وخبراء الأدلة الرقمية يواجهون تحديات مع شركات تقنية متطورة جداً ومختلفة المنتجات لذا يجب المسارعة في إنشاء مركز معلومات وطني للأدلة الرقمية وجرائم التقنية والحاجة لإيجاد نظام معياري للتعامل مع الأدلة الرقمية.

متطلبات خبراء الأدلة الرقمية

تقنيات سريعة في المعالجة وتكامل البيانات، وتدريب مستمر حسب منتجات شركات التقنية، ومشاريع وطنية تقنية تخدم (تطبيقات) اللغة العربية وأنظمة تحليل آلي وتكامل البيانات بين جهات معالجة الأدلة الرقمية.

الهواتف النقالة :- أماكن العثور على الأدلة الإلكترونية

في مسرح الحادث. ومع المجني عليه أو الجاني وعلى الشبكة المحلية

أين يمكن العثور على الأدلة الرقمية في الهواتف النقالة ؟

أولاً :– يمكن تخزين البيانات في (3) مواقع

شريحة الاتصال. كرت الذاكرة. الهاتف النقال

ثانياً :– بعض البيانات يمكن أن تخزن في أكثر من موقع

– سجل الأسماء يكون في شريحة الاتصال أو جهاز الهاتف النقال.

– الصور تكون في جهاز الهاتف النقال أو كرت الذاكرة ((Integrated Circuit Card Identifier (ICCID) هو رقم تعريف للشريحة عبارة عن رقم يتكون من عشرين خانة – دائماً يخزن رقمياً في البطاقة ولا يمكن تعديله – ويكون مطبوع على الشريحة. – يمكن تحديد مزود الخدمة والدولة من خلال ICCID رقم تعريفي :- International Mobile Equipment Identifier (IMEI) عبارة عن رقم يتكون من 15 خانة تخزن رقمياً في أجهزة الهواتف النقالة مطبوع على اللاصق تحت البطارية يمكن تحديد صناعة الجهاز وموديله من خلال (IMEI).

طريقة الاتصال بين الأجهزة النقالة وأجهزة الفحص

1– الكيابل (Cable) / – أسرع وأمن البلوتوث (Bluetooth) / أقل سرعة وأمان

الأشعة تحت الحمراء (Infra - red) / بطيء أمن قد تختلف النتائج عند قراءة جهاز الهاتف النقال بطرق مختلفة.

هنالك طريقتين لاستخراج البيانات :

استخراج البيانات بطريقة Extraction يتطلب كيابل وبرامج خاصة. – يقدم الكثير من البيانات من ضمنها البيانات المحذوفة.

مميزات أجهزة الهواتف النقالة / (أصغر أخف. أسرع. أرخص. تستهلك طاقة أقل. زيادة في عدد الوظائف).

ماذا يمكن لمزودي الخدمة أن يزوده لجهات التحقيق ؟

* معلومات المواقع

* سجل المكالمات الواردة / الصادرة.

* الرسائل النصية، رسائل الوسائط

* IMEI/ IMSI/ ICCID

* البريد الصوتي، رقم الاتصال، PUK code

* تفاصيل المشترك (الاسم – العنوان – ... إلخ).

* تفاصيل الدفع (بطاقة الائتمان – الحساب البنكي).

* عمل شريحة مماثلة واستخراج البيانات من الجهاز (SIM ID Cloner) يفقد سجل المكالمات عند تغيير شريحة الاتصال أكثر أجهزة الهواتف النقالة سوف تقوم بحذف سجل المكالمات المخزن بها عند إدخال شريحة اتصال مختلفة كروت الذاكرة.

* توجد أشكال مختلفة من كروت الذاكرة حسب المصنع مثل MMC, micro SD, Memory Stick M 2 ... إلخ.

* الآن متاح ذاكرة سعة 64 GB

* تعتمد على نظام ملفات FAT file system

* ربما تحتوي على صور، مقاطع فيديو، ملفات صوت أو ملفات أخرى، أجهزة الهواتف النقالة ذات طابع مختلف جداً.

* هناك اختلاف شاسع بين أجهزة الهواتف النقالة المختلفة : الشكل، منفذ البيانات، مداخل الشواحن، الملامح، المميزات، الذواكر ... إلخ.

*كل أجهزة الجوال يجب أن تحتوي على رقم تعريفي فريد (IMEI (International Mobile Equipment Identifier لماذا عملية SIM ID Cloner) نحتاج لعزل الجهاز عن الشبكة لمنع المكالمات / الرسائل الواردة.

* بعض أجهزة الجوال تحتاج إلى شريحة اتصال لإتمام عملية الفحص في المقابل.

* عند تمكين جهاز الاتصال بالشبكة : - تغيير في سجل المكالمات والرسائل النصية – الملفات المحذوفة قد يتم الكتابة عليها في هذه الحالة – يمكن مسح كافة البيانات نهائياً باستخدام وسيلة wiping في الهواتف من خلال بعض البرامج المطبقة في الأجهزة الذكية.

حماية الشريحة بالرقم السري PIN

* أغلب بيانات شريحة الاتصال يمكن حمايتها بشكل اختاري بالرقم السري (4 – 8 digit PIN).

* المستخدم يستطيع تغيير الرقم السري، إدخال الرقم السري بشكل خاطئ ثلاث مرات سيحجب الشريحة Personal Unblocking Key (PUK).

* رفع الحجب عن الشريحة عبارة عن (8 - digits) وهو مفتاح رفع الحجب الشخصي (PUK).

* PUK code يكون معروف لدى مزودي الخدمة (لا يمكن تغييره عن طريق المستخدم).

* بعد إدخال PUK بشكل خاطئ عشرة مرات سيتم تعطيل الشريحة الوصول للرقم السري لجهاز الهاتف النقال.

* متاح لمئات الأجهزة وتحتاج إلى كيابل خاصة .

- iDevices

– الرقم السري مكون من أربع خانات 4 digit passcode

– جميع أجهزة وبرامج الفحص تدعم iPhone 3 GS, 4 CDMA, 4 GSM, iPod touch 3G and 4 and iPad والانتقال من موقع لآخر، الهاتف وشبكة الاتصال على تواصل بشكل دوري (تحديث) ليمكن الوصول إلى الهاتف.

– شريحة الاتصال تبقى تسجيل للموقع (Location Area Code (LAC.

– مزود خدمة الاتصال يمكنه تزويد (جهات التحقيق) بمعلومات أكثر عن معلومات المواقع بالرجوع لـ (cell site)، الهواتف تراقب بصفة دورية قوة إشارة الاتصال وتسجل بصمة لها على الموقع.

مركز الإنتربول لمكافحة الجريمة الرقمية :- الاستفادة من الأدلة الجنائية الرقمية [1].

في الوقت الذي يستغل فيه المجرمون التكنولوجيا الحديثة وسهولة السفر من بلد لآخر وإمكانية إخفاء هوياتهم عند استخدام الإنترنت، يتعين على أجهزة الشرطة والجهات الشريكة في القطاع الخاص تكييف الإجراءات التي تعتمدها لمواجهة هذا النمط الإجرامي الجديد والمتنامي مواجهة فعالة.

ففي الماضي، عندما يسطو أحد الأشخاص على مصرف ما، كانت قائمة المشبوهين تقتصر على الأشخاص الذين يدخلون المصرف، أما في يومنا هذا، عندما يتعرض مصرف لعملية سطو رقمي، يمكن أن يصبح أي شخص يستخدم جهاز حاسوب موصولاً بالإنترنت مشبوهاً محتملاً، وفي العالم الافتراضي، يمكن تقريباً لأي شخص أن تكون له صلة بجريمة ما وأن يتمكن من محو أي أثر لأنشطته، في حين أن هذا أمراً شبه بالمستحيل في العالم الواقعي.

ولم تعد أجهزة الشرطة تكتفي ببساطة بتحديد الصلات بين الجريمة والمجرمين على الصعيد الوطني، ولكن أصبح يتعين عليها تعقب المجرم عبر سلسلة من الشبكات المتشعبة التي تنتشر في بلدان عديدة في أغلب الأحيان لذا، تصبح الأدلة الجنائية الرقمية جزءاً لا يتجزأ من أي تحقيق، إذ تتيحل لشرطة تعقب مشبوه ما والكشف عن هويته وإعداد ملف جنائي ضده.

وسيبني مجمع الإنتربول العالمي للابتكار، بفضل مختبر الأدلة الجنائية الرقمية التابعة، القدرات الوطنية في مجال الأدلة الجنائية الرقمية مستفيدا في ذلك من خبرات الجهات المعنية المتعددة، لتزويد المحققين بالتكنولوجيا والمهارات العملية اللازمة لتنسيق التحقيقات في الجرائم الرقمية عبر الوطنية وسوقها على نحو أفضل الأنشطة الرئيسية.

سيتعاون مجمع الإنتربول العالمي للابتكار مع خبراء من القطاعين العام والخاص ومن الأوساط الأكاديمية لتوفير كل ما يلزم من أدوات وبيانات استخبار وخبرات في مجال الأدلة الجنائية الرقمية من أجل مكافحة الجريمة السيبرية بمزيد من الفعالية.

وستتركز هذه الأنشطة في مختبر للأدلة الجنائية الرقمية الذي سيوفر دعماً شاملاً لأجهزة الشرطة الوطنية في العالم أجمع.

تحليل برامج الحاسوب الإجرامية

(1) موقع الأنتربول – المجمع العالمي للابتكار.

1- سيحلل مختبر الأدلة الجنائية الرقمية البرمجيات الخبيثة وغيرها من الأدوات المستخدمة في ارتكاب الجرائم السيبرية) برامج الحاسوب الإجرامية (التي يكشف عنها الإنتربول.

2- أو يحيلها بلد عضواً أو منظمة شريكة.

3- وسترسل التقارير التحليلية عن البرمجيات الخبيثة إلى البلدان الأعضاء لكي تتمكن من تنسيق الإجراءات المتبعة للتحرك على الصعيد الوطني وتعيد توزيع مواردها.

4- وسيرصد المختبر أيضاً اعتداءات برمجيات "البوتنت" الخبيثة وتحليل الروابط بين الأنشطة الضارة لتتبع خيوط هذه الأنشطة وصولاً إلى الجناة في نهاية المطاف.

الأدلة الجنائية المتصلة بالأجهزة النقالة :-

تشغل أعداد هائلة من الأجهزة النقالة الجديدة كالعام في جميع أنحاء العالم، فتزداد الحاجة إلى تركيز الجهود والأنشطة في مجال الأدلة الجنائية المتصلة بالأجهزة النقالة. وتوفر مختلف شركات القطاع الخاص التدريب والأدوات اللازمة لتمكين الموظفين من تحليل هذه الأدلة الجنائية لأن هم يدركون أهمية جمع الأدلة الرقمية واستخراجها من هذه الأجهزة دون المساس بالبيانات.

وبالتالي، سيستفيد المجمع العالمي من الخبرات والأدوات التي يوفرها شركاؤه من القطاع الخاص، الأمر الذي سيعود بفائدة كبرى على البلدان الأعضاء في التحقيقات التي تجريها وبرتوكولات معاملة الأدلة التي تطبقها وفهمه العامل مجال بيانات الأدلة الجنائية.

وسيستخدم مختبر الأدلة الجنائية أحدث التقنيات والحلول في هذا المجال لمساعدة البلدان الأعضاء على فحص الأجهزة الرقمية من أجل ضمان تحليل الأدلة الجنائية بانتظام.

اختبار أدوات الأدلة الجنائية

سيضطلع مختبر الأدلة الجنائية الرقمية بأنشطة أخرى تهدف إلى تبيان الأدوات التجارية وغير التجارية لفحص الأدلة الجنائية الرقمية، التي يطورها القطاع الخاص والأوساط الأكاديمية ومختبرات البحوث الوطنية وسيجرب المختبر لاحقاً بالتعاون مع أطراف أخرى هذه الأدوات البالغة التطور والخدمات والبروتوكولات وسيساعد في إطلاقها وتنسيقها، من أجل توسيع نطاق مكافحة الجريمة السيبرية والتشجيع على استخدام الأدلة الجنائية الرقمية على الصعيد الوطني.

وسيشرك الإنتربول أيضاً على نحو استباقياً لجهات المعنية الإستراتيجية، ولاسيما مختبرات ومعاهد البحوث والأوساط الأكاديمية والقطاعين العام والخاص، في عملية استنباط وتصميم ابتكارات تكنولوجية متطورة للتصدي للأنشطة الإجرامية السيبرية في الوقت الحالي وفي المستقبل.

التدريب على الأدلة الجنائية الرقمية

سعيد مختبر الأدلة الجنائية الرقمية ويوفر دورات للتدريب على التطور المهني، توجه للخبراء في مجال فحص الأدلة الجنائية والمحققين وغيرهم من الأشخاص الذين يتدخلون فور وقوع جرائم رقمية، وذلك للتحقق من امتلاكهم آخر المعارف المتصلة باتجاهات الجريمة السيبرية، ومن قدرتهم على استخدام أدوات فحص الأدلة الجنائية الرقمية وتقنياتها.

وسيوفر المختبر أيضاً التدريب على فحص الأدلة الجنائية المتصلة بالحواسيب والأجهزة النقالة البرمجيات الخبيثة، وعلى أحدث الأدوات التكنولوجية والتقنيات في مجال الأدلة الجنائية الرقمية.

وسيدير أيضاً مركزاً للمعارف يجمع مواد التدريب التي يمكن للبلدان الأعضاء أن تطلع عليها لتسهيل تبادل المعلومات وتحديد أفضل الممارسات المتعلقة ببناء القدرات في مجال الأمن السيبيري.

وأخيراً المجرم المعلوماتي / الجريمة الحاسوبية

يتميز المجرم المعلوماتي عن المجرم التقليدي بأنه مجرم على درجة عالية من العلم والتخصص والمهارة، لكنه يستغل تلك الصفات استغلالاً غير مشروع.

وتتميز الجريمة الحاسوبية عن الجريمة التقليدية بأنها تتم في الخفاء في بيئة حاسوبية مكوناتها برمجيات وأجهزة حاسوب وشبكات معلومات.

وعلى خلاف الجريمة التقليدية، يصعب الحصول على أدلة مادية، وتستلزم طرقاً خاصة حديثة لإثباتها، هذه الجرائم لا يحدها مكان أو زمان. ووقت تنفيذها قد لا يستغرق بضع دقائق.

أدلة الجرائم الحاسوبية تشمل سجلات الكمبيوتر ومعلومات الدخول والخروج والاشتراك ومواد رقمية مستوحاة من أجهزة حاسوب أو ملحقاتها أو شبكاتها، يتم تجميعها وتحليلها باستخدام أنظمة متطورة حديثة ويتم تقديمها كأدلة يمكن الاعتماد عليها أمام القضاء. وقد أثارت وتثير أمام القضاء مشكلات جمة من حيث مدى قبولها وحجيتها.

في أدلة الجرائم الحاسوبية يمكن استخراج نسخ احتياطية من تلك الأدلة مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية (بشرط أن تتم وفق أسس وقواعد متفق عليها عالمياً) بعكس أدلة الجرائم التقليدية.

وأيضاً يمكن الاستعانة بخبير ذو خبرة علمية وعملية بموضوع الجريمة أو بجزء منها وباللغة الإنجليزية يسمى expert witness يستعين به رجل القانون كإجراء في جمع الأدلة كي تنير الطريق في السعي لتحقيق العدالة، وندرك أن اختصاص القضاء بخصوص الجرائم الحاسوبية والقوانين الواجب تطبيقها لا تحظى دائماً بالوضوح أو القبول أمام حقيقة أن غالبية هذه الجرائم ترتكب من قبل أشخاص من خارج حدود الدولة أو أنها تمر عبر شبكات معلومات خارج حدود الدولة رغم ارتكابها من قبل أشخاص داخل حدود الدولة للاعتداء على أنظمة داخل حدود الدولة المعنية بالجريمة [1].

9- الخاتمة

رافق الثورة الصناعية منذ منتصف القرن الماضي تطورات وتبدلات بسائر جوانب الحياة في المجتمع فانعكست متطلبات تلك الثورة على المعلومات التي زادت غزارتها وضخامة عدد كتبها ووثائقها لدرجة بات معها أمر حفظها وتخزينها يستلزمان مكتبات كثيرة وأماكن واسعة، وتصنيفها وتبويبها يتطلبان وقتاً وجهداً كبيرين والرجوع إليها لا يقل عن ذلك جهداً ووقتاً.

فكان لابد من التفكير بوسيلة يتم من خلالها تجاوز هذه المشكلات، على أن ظهر الحاسوب وبدأ بالعمليات الحسابية، ثم تطور ليشمل أعمال التخزين واستيعاب كبير للمعلومات، وتجميعها وترتيبها واسترجاعها بسرعة فائقة ودقة متناهية فصارت المعلومات في متناول الأيدي بجهد بسيط ووقت طويل.

هذه الميزات العالية جداً للحاسوب الإلكتروني جعلت الاستعانة به واستخدامه ضرورة لا غنى عنها لدى أجهزة الدولة والأشخاص الاعتباريين والعاديين، مما جعل الحاسوب يفرض نفسه في كافة المجالات.

نتيجة ذلك ظهرت إلى حيز الوجود علاقات استثمارية جديدة، بعضها انصب على تصنيع الحاسبات وآخر على إعداد البرامج اللازمة لمعالجة المعلومات، وإعداد الكوادر الفنية المتخصصة في أعمال الحاسوب إضافة لدخول الحاسوب نفسه كسلعة جديدة في مجال التداول التجاري.

ظهور هذه العلاقات رافقه ظهور لعلاقات قانونية جديدة، لم تكن معروفة من ذي قبل، ولدى قيام المنازعات بشأنها، وقفت النصوص القانونية السائدة قاصرة، إن لم تكن عاجزة، عن هذه المنازعات والجرائم، خاصة مع بروز الجريمة المعلوماتية إلى حيز الوجود / فالجريمة المعلوماتية قوامها أحد السببين التاليين -:

أن تكون المعلوماتية، وسيلة للغش والتحايل والاعتداء أن تكون المعلوماتية نفسها محلاً للاعتداء ... والجريمة الالكترونية هي " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها". وتتمثل الجريمة الالكترونية في كل فعل أو سلوك سيء غير مشروع مرتبط بأجهزة الحاسب الآلي مما قد يسبب خسارة للمجني عليه وإمكانية حصول مرتكب هذه الجريمة على أية ربح أو مكسب. وغالباً ما تهدف هذه الجرائم الإلكترونية إلى الحصول على معلومات سرية أو تغيير وتزوير بعض المعلومات أو حتى إفساد الأجهزة الإلكترونية وتعطيلها.

المراجع

[1] القرآن الكريم والسنة المطهرة على صاحبها أفضل الصلاة والتسليم.

[2] المعجم المفهرس لألفاظ القرآن الكريم؛ المؤلف، محمد فؤاد عبد الباقي؛ حالة الفهرسة: مفهرس على العناوين الرئيسية: الناشر: دار الكتب ... الناشر: دار الكتب المصرية – سنة النشر: 1364 هـ.

[3] موقع هيئة الاتصالات وتقنية المعلومات / المملكة العربية السعودية و الموسوعة الحرة.

[4] موقع الإنتربول – المجمع العالمي للابتكار وموقع المنظمة العربية لتنمية الإدارية /

[5] الأدلة الإلكترونية للجرائم الحاسوبية / موقع الخبراء العرب وموقع الصحيفة الإلكترونية.

[6] وحدة خدمات الإنترنت / موقع مدينة الملك عبد العزيز للعلوم والتقنية وموقع الاتحاد العالمي لعلماء الإسلام.

[7] المعلومات الأمنية / اللواء د. محمد فاروق عبد الحميد كامل – أكاديمية نايف العربية للعلوم الأمنية (جامعة نايف حالياً) بالرياض – 1420 هـ الموافق 1999 م.

[8] (*) – أرشيف قانونية / منتديات ستار تايمز – الدليل الرقمي في مجال الإثبات الجنائي / أ. طارق محمد الجملي عضو هيأة التدريس بكليات القانون – جامعة قاريونس.

[9] باختصار / رابط الموضوع: http://www.alukah.net/culture.

[1] الأدلة الإلكترونية للجرائم الحاسوبية / موقع الخبراء العرب.

[10] جرائم الحاسب الآلية. الرياض: محمد محمود مندورة – مكتب الآفاق المتحدة 1410 هـ.
[11] لسان العرب / أبو الفضل، جمال الدين ابن منظور الأنصاري الرويفعي الإفريقي (المتوفى : 711 هـ).
[12] موقع صيد الفوائد باختصار، موقع المسلم، موقع السكينة.
[13] www.almaaref.org/books/contentsimages/booksl
[14] مدونة / منشورة على الشبكة – حقيقة كاتبها يشكر عليها أوجز وأكمل مدونة – أبو عبد العزيز / سليمان بن صالح المطرودي / الرياض – 1435 / 6/ 6 هـ - مرسلة بواسطة Sulaiman Al – Matrudi في 48 : 22 – بتصرف بسيط.
[15] موقع الشيخ / د. إبراهيم بن محمد الحقيل / مقتطفات من خطبة بعنوان أجهزة التواصل الاجتماعي نهر بر وخير في بحر اثم وشر – رابط الموضوع : http://www.alukah.net/sharia.
[16] 16- جريدة الرياض / الأربعاء أ ذي القعدة 1435 هـ - العدد 16865 – تحقيق وتقارير مسؤولية المجتمع يتجاوز أخطاءه ويمضي مع أبنائه إلى الأمام بوعي وبلا تردد – باختصار وأعداد أخرى مبينه في الهوامش.
[17] مقتطفات من ندوة المجتمع والأمن – دورة (5) كلية الملك فهد الأمنية بالرياض – الجرائم اليكترونية الملامح والأبعاد.-5-7/ربيع الثاني/1428هـ الموافق 22-24/ ابريل 2007م.
[18] تحديات التحقيق في الأدلة الرقمية – د. فهد بن عبد الرحمن الشثري / ورشة الأدلة الرقمية بنادي الضباط – بالرياض 1434 هـ.
[19] جرائم الهواتف النقالة / الإدارة العامة للأدلة الجنائية.
[20] الظواهر الإجرامية المستحدثة وسبل مواجهتها – أكاديمية نايف العربية للعلوم الأمنية (جامعة نايف العربية للعلوم الأمنية – حالياً) ندوة علمية عقدت في تونس في الفترة من 14- 16/ 3/ 1420 هـ الموافق 28 / 6/ 1999 م / المبحث الثالث – جرائم الحاسب والإنترنت – د. ذياب موسى البداينة.